



UNITED STATES PATENT AND TRADEMARK OFFICE

MN
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|--------------------------------|------------------------|
| 10/629,175 | 07/29/2003 | Alan D. Boulanger | RPS920030010US1 | 7176 |
| 26675 7590 08/03/2007 DRIGGS, HOGG & FRY CO. L.P.A. 38500 CHARDON ROAD DEPT. IRA WILLOUGBY HILLS, OH 44094 | | | EXAMINER AVELLINO, JOSEPH E | |
| | | | ART UNIT 2143 | PAPER NUMBER |
| | | | MAIL DATE 08/03/2007 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/629,175

Applicant(s)

BOULANGER ET AL.

Examiner

Joseph E. Avellino

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 May 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 8-12, 16-22, 25, 26, 30, 34 and 35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 8-12, 16-22, 25, 26, 30, 34 and 35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-4, 8-12, 16-22, 25, 26, 30, 34, and 35 are presented for examination; claims 1, 11, 20, 25, and 30 independent. The Office acknowledges the cancellation of claims 5-7, 13-15, 23, 24, 27-29, and 31-33.

Claim Rejections - 35 USC § 101

2. The Office has considered the amendments to the claims. The rejection under 35 USC 101 is hereby withdrawn.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 2, 8-12, 16-22, 25-26, 30, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin et al. (USPN 6,487,666) (cited by Applicant in IDS) (hereinafter Shanklin) in view of Tarquini et al. (US 2003/0101353) (hereinafter Tarquini).

4. Referring to claim 1, Shanklin discloses a method for detecting unauthorized reconnaissance or scanning (i.e. detect attacks on a local network) of a computer network comprising the acts of:

monitoring communications within the network (col. 1, lines 27-32);

detecting predefined sequence of packets flowing within communications (i.e. packets of a specific type in a specific order which satisfy a prescribed expression) (col. 5, lines 23-40; col. 6, lines 15-20); and

issuing an alert indicating unauthorized scanning if the predefined packet sequence is relevant to a specific source address (i.e. an alarm is generated) (col. 6, lines 15-20).

Shanklin does not explicitly state that the sequence of packets is a SYN from a source address to a target device, a SYN/ACK from a target back to a source address, and then a RST packet in response to the SYN/ACK, rather that an expression can be created by using packet types represented by A, B, and C (col. 5, lines 25-30). In analogous art, Tarquini discloses another intrusion detection system which describes the well known predefined sequence known as a TCP SYN scan, wherein a predefined triplet of a SYN packet is sent to a desired port, in the event that a SYN/ACK is received, the system immediately transmits a RST to tear down the connection (§ 44). It would have been obvious to one of ordinary skill in the art to combine the teaching of Tarquini with Shanklin in order to create an expression in order to detect the TCP SYN scan, since Shanklin disclose that the expression shown at col. 5, line 29, defines three packet types A, B, and C. One of ordinary skill in the art would realize the benefits of creating an expression in the system of Shanklin in order to detect a TCP SYN scan in progress, thereby further enhancing the intrusion detection system of Shanklin.

Art Unit: 2143

5. Referring to claim 2, Shanklin discloses the monitoring is done with a selected network device (i.e. intrusion detection system sensor 11) (col. 2, lines 35-45).

6. Referring to claim 8, Shanklin discloses sending a message to an administrator (i.e. report the attack) (col. 1, lines 35-38).

7. Referring to claims 9 and 10, Shanklin does not specifically disclose blocking future packets from network computers having predefined characteristics, or rate-limiting flows of packets, however these are common preventative measures to ensure an attack on a network is not successful. By this rationale, "Official Notice" is taken that both the concepts and advantages of providing for blocking or rate limiting packets is well known and expected in the art. It would have been obvious to one of ordinary skill in the art to modify the teaching of Shanklin to include blocking or rate-limiting packets, since Shanklin discloses the use of firing an alarm, however does not specifically discuss what the alarm does. This would lead one of ordinary skill in the art to search the art to find methods of network defense, eventually finding the well known features of rate-limiting and blocking packets from specific addresses.

8. Claim 12 is rejected for similar reasons as stated above.

9. Referring to claim 13, Shanklin-Tarquini discloses the invention substantively as described in claim 11. Shanklin does not disclose the actual values of the state codes

of the table in which the packets are observed, however Shanklin does disclose monitoring a particular sequence of packets (col. 5, lines 13-33). Therefore there inherently must be a mechanism within Shanklin which is capable of determining if the particular sequence of packets fits this particular "signature" (i.e. a sequence of packet type A, followed by 0 or more packets of any type, followed by two packets of type B, followed by 0 or more packets of any type, followed by a packet of type C, will match the expression A.*BB.*C as given in an example in col. 5, line 29. Therefore the computer must be able to determine when a first of the sequence, a second of the sequence, and the last of the sequence of predefined packets has been received. The state codes chosen do not provide any patentable distinction and are mere design choice.

10. Claims 16-22, 25-26, 30, 34, and 35 are rejected for similar reasons as stated above.

Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin-Tarquini in view of Etheridge et al (US 20040054925) (hereinafter Etheridge).

11. Referring to claim 3, Shanklin discloses the invention substantively as described in claim 1. Shanklin further discloses counting a particular type of packet in a certain time period in order to determine whether to fire an alarm (i.e. if SYN packet count >50 within Time, FireAlarm) (col. 6, lines 15-20). Shanklin does not specifically disclose providing a histogram to maintain the states of the sequence of packets, and update the

histogram as the packets are detected. In analogous art, Etheridge discloses another system for detecting network attacks which uses a histogram to monitor which packet types are incoming, and updates the histogram when the packet arrives (p. 7, ¶ 83-84). It would have been obvious to one of ordinary skill in the art to combine the teaching of Etheridge with Shanklin, since it would provide an efficient method for the system of Shanklin to monitor the reception of packets and fire alarms when needed.

12. Referring to claim 4, Shanklin in view of Etheridge discloses the invention substantively as described in claim 3. Etheridge further discloses a second field which a code representing states in which packets in the predefined sequence are detected (i.e. the histogram corresponding to TCP is incremented) (p. 7, ¶ 84). Shanklin-Etheridge do not specifically disclose that the histogram tracks the source addresses of the network devices, however Shanklin does disclose that the rule of counting SYN packets is *for any one host* (col. 6, lines 15-20). By this rationale, one of ordinary skill in the art would rationally assume that the source address must be somewhat correlated to the current count of SYN packets, in order to allow the scanner 11 the ability to determine whether or not the SYN packet is part of the affected rule for a particular sender or another sender who is a verified user who should not be penalized.

Response to Arguments

13. Applicant's arguments dated May 30, 2007 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant has failed to seasonably challenge the Examiner's assertions of well known subject matter in the previous Office action(s) pursuant to the requirements set forth under MPEP §2144.03. A "seasonable challenge" is an explicit demand for evidence set forth by Applicant in the next response. Accordingly, the claim limitations the Examiner considered as "well known" in the first Office action, are now established as admitted prior art of record for the course of the prosecution. See *In re Chevenard*, 139 F.2d 71, 60 USPQ 239 (CCPA 1943).

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

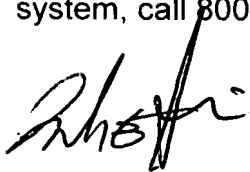
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph E. Avellino whose telephone number is (571) 272-3905. The examiner can normally be reached on Monday-Friday 7:00-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Joseph E. Avellino, Examiner
June 1, 2007